The Odisha Gazette

EXTRAORDINARY
PUBLISHED BY AUTHORITY

DEPARTMENT OF AGRICULTURE & FARMERS' EMPOWERMENT
DIRECTORATE OF AGRICULTURE & FOOD PRODUCTION, ODISHA
KRUSHI BHAWAN, BHUBANESWAR-751001
NOTIFICATION
The 12th August, 2024

[No.28167—DAFP-SPII-MISC-0063/2022/Agril.]

Background:

The Government of Odisha has been consistently working towards the welfare of the farmers in the state. The increase in production of paddy witnessed in the last couple of decades is a testament to the efforts made by the government. Building upon the work to digitize and streamline service delivery over the past couple of years, the Department of Agriculture and Farmers' Empowerment (DAFE) has begun an ambitious project to unify all the digital infrastructure and build a one stop solution i.e. a unified portal/app for the farmers (FUP/Krushak Odisha App). The FUP will consist of Unified Farmers' Services Interface (UFSI) which will act as an interface for the different govt. systems and ecosystem partners to communicate with one another and seamlessly provide services to the farmers via the FUP.

The objective of the KONNECT stack (Figure 1) Is to facilitate and leverage partners along the agriculture value chain such as financial institutions, input suppliers, traders, Agri-Entrepreneurs, Agri-Tech organizations for the welfare of farmers in the state. To achieve the objectives, a robust and stringent data sharing framework is proposed to allow fair and secure transactions between the farmers and the ecosystem partners on the stack.

About KONNECT Stack:

KONNECT stack creates an open ecosystem platform that makes the markets work for farmers and lets the agri-value chain operate at a higher equilibrium by reducing information asymmetry and increasing choices for farmers. The stack:

1. Creates a platform which can be leveraged to link farmers, policy makers, buyers, and farm service providers by creating simple service provider and farmer-facing UIs and leverage standardized API specifications.

2. Enables services for farmers across
    a. Farm inputs
    b. Credits
    c. Market
    d. Extension

3. Farmer data across state agriculture database (eg. Krushak Odisha database) and other federated data can be consumed in an owner-consented and secure manner.

Figure 1: Framework of KONNECT stack
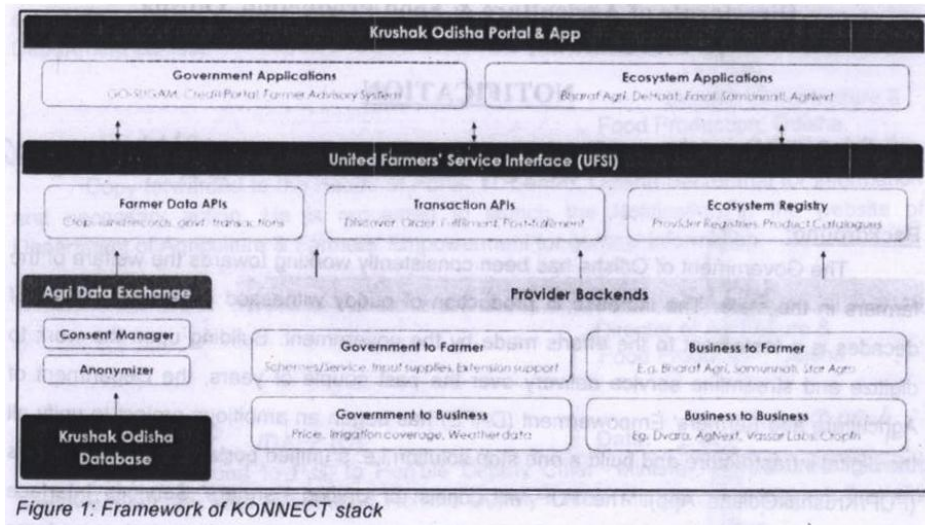
Purpose of Data Sharing Framework:

The S&T department had notified the Odisha State Data Policy (OSDP) in the year 2015 under the supervision of ORSAC. The main objectives of the OSDP was to facilitate storage and access of government acquired data, improve accessibility of data to all stakeholders, ensure timely availability of data for disaster management and empower stakeholders to take data backed decisions, reviews and monitoring.

While the policy effectively facilitated the public availability of government-acquired data on the portal, it could have further enhanced its focus on prioritizing privacy and consent when sharing such data with ecosystem stakeholders. It also did not outline any framework for consent while collecting or processing personal data nor did lay down the process and workflow for obtaining the consent from the citizens.

Hence, there is a need to formulate a data sharing framework that will protect privacy and ensure secure flow of data on the stack in line with the provisions of "Information Technology Act" of 2000, "National Data Sharing and Accessibility Policy" (NDSAP) of 2012, Aadhaar Act of 2016, and the "The Digital Personal Data Protection" (DPDP) Act of 2023.

This framework is the first step in realizing the stack's principle of "Security and Privacy by Design" for the protection of farmer's personal data privacy. It acts as a guidance document across the stack and sets out the minimum standard for data privacy protection that should be followed across the board in order to ensure compliance with relevant and applicable laws, rules and regulations. This framework will be dynamic in nature and may be revised from time to time as may be required by competent authority.

This framework is to be read along with, and not in contradiction to, any applicable law, or any instrument having the effect of any law together with the Blueprint, policies relating to information security, guidelines relating to data retention and archival, or any other policies or guidelines which may be notified from time to time.

Applicability of this framework:

The provisions of this framework shall be applicable to all the entities and individuals who are part of the KONNECT stack or in other words are part of the FUP either as service providers or beneficiaries. Illustrative list is as follows:

a) All farmers who voluntarily use the services and transact on the stack via FUP
b) All government departments or entities that are acting as data providers in the ecosystem.
c) All individuals, teams, entities or private ecosystem partners who collect or process data of any individual as part of the stack.
d) All methods of contact, including in person, written, via Internet, telephone, as the case may be.

Objectives:

The key objectives of this framework are:

a) To provide adequate guidance and to set out a structure for the secure processing and sharing of personal and sensitive data of farmers in compliance with all applicable laws.
b) To safeguard digital personal data within the ambit of this framework and create a system of datasets which is easily accessible to farmers and ecosystem service providers based on the consent of farmers, and in compliance with relevant standards.
c) To leverage the information systems existing in the DAFE and F&ARD by encouraging conformity with the defined data privacy standards and integrating such existing systems.
d) To increase awareness of the importance of data privacy and instill a privacy-oriented mindset among the farmers and the ecosystem partners.
e) To provide a data monetization mechanism to leverage open data to address social challenges and provide public benefits. This may include using revenue generated from open data to fund social programs, initiatives, or public services that benefit communities.

Definitions:

a) **"Data Fiduciary"** means a company or government department within the ecosystem which alone, or in conjunction with others, determines the purpose of processing of data and makes a request to obtain the consent. For the purpose of this framework, data fiduciaries would include banks, insurers, govt. departments, private ecosystem partners etc.

b) **"Anonymization"** means the process by which an entity may remove, or mask personal identifiers from data, or replace them with such other fictitious name or code that is unique to a farmer but does not, on its own, directly identify the farmer.

c) **"Consent Artifact"** is a machine-readable electronic document that specifies the parameters and scope of data that a user consents to in any data sharing transaction. In this framework, consent must be digitally signed, either by the user or by the consent collector or both

d) **"Agriculture Data Exchange (AgriDex)"** is a Data Empowerment And Protection Architecture (DEPA) compliant data fiduciary block that enables farmer consent driven access to data for third-party data requesters. Implementation Structure:

Figure 2: Consent Implementation Structure
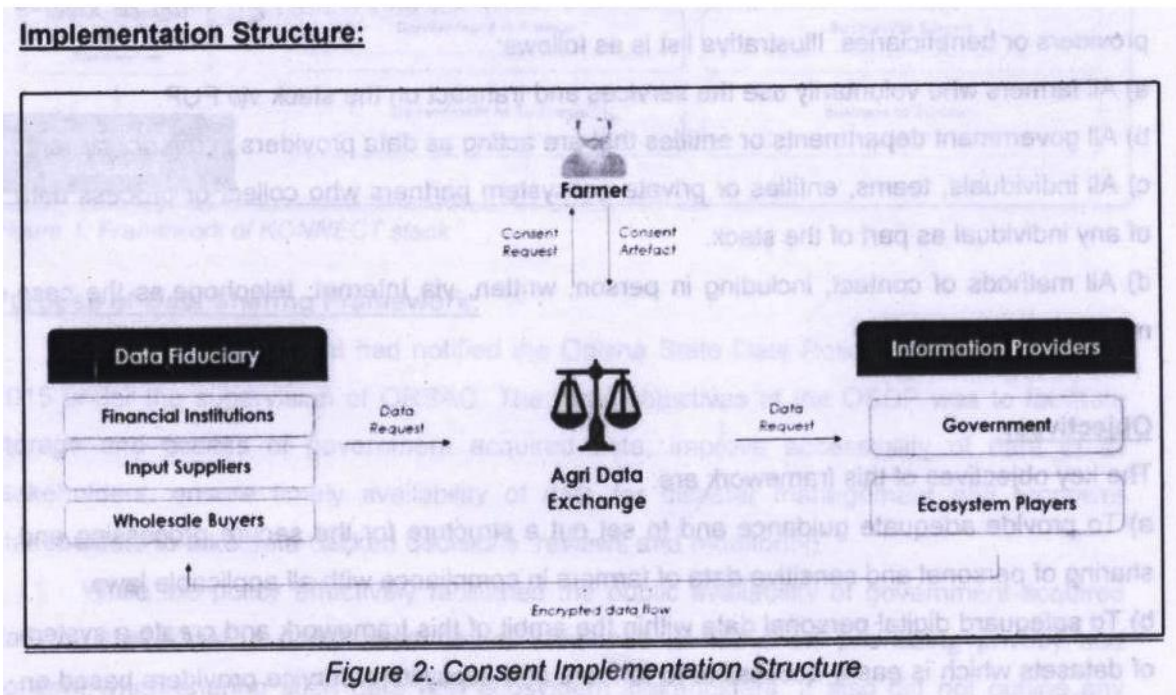
Consent Mechanism:

1.Collection of Data by Data Fiduciaries

Data fiduciaries can collect anonymized data, which shall be limited to such data that is necessary for the purposes under the umbrella of the stack. Aadhaar data must be shared with

proper authorization in line with the existing practices and for only those purposes as permitted in the Aadhaar Act.

2. General Principles Governing Consent Framework

The consent framework under this should incorporate the following principles in relation to processing of data by data fiduciaries:

a) Farmers should at all times have control and decision-making power over the manner in which data associated with them is collected and processed further.

b) Specifically, in the case of electronic consent, data fiduciaries should make use of appropriate technological means to prevent security breaches and to guarantee integrity of access permissions given by farmers. Such technological means must be in conformance with the relevant national and international standards.

c) So far as sharing or disclosure of any data is concerned, the technical design of the consent management framework should also ensure interoperability across all players of the KONNECT stack. The framework should be agnostic to applications, programming languages, and platforms.

3. Consent in relation to Collection and Processing of Data

3.1 Data fiduciaries can collect or process anonymized data only with the consent of the farmers. It is the responsibility of the data fiduciary to ensure that the consent given by the farmers is valid.

3.2. The consent of the farmer will be considered valid only if it is:

a) Free, having regard to whether it complies with the standards set out under Section 14 of the Indian Contract Act, 1872.

b) Informed, having regard to whether the farmer has been provided with the necessary information by way of notice, as set out in clause 4 of this framework, the scope of consent in respect of the purpose of processing.

c) Specific, where the farmer can give consent for the processing of anonymized data for a particular purpose.

d) Capable of being withdrawn at any time, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

3.3. In addition to the conditions mentioned in Clause 3.2 above, the consent of a farmer in respect of collecting or processing any data will be obtained only after informing her/him the purpose of collecting such data.

4. Privacy Notice for the Collection or Processing of Data

4.1. All data fiduciaries must give a clear and conspicuous privacy notice to the farmers

a) prior to the collection of data from the farmer.

b) at the time the data fiduciary changes its privacy policies or procedures.

c) prior to the collection or further processing of data of the farmer for any new or previously unidentified purpose.

4.2. It is clarified that for the purpose of Clauses 4.1(b) and (c) above, all data fiduciaries must obtain fresh consent from the farmer in accordance with the consent mechanism. The privacy notice should contain the following information:

a) The purposes for which the data is to be processed;

b) The nature and categories of data being collected by data fiduciary.

c) The methods or mechanisms by which the data is collected by the data fiduciaries

d) The identity and contact details of the data fiduciary collecting the data;

e) The right of the farmer to withdraw her/his consent, and the procedure for such withdrawal:

f) The individuals or entities along with their contact details, including other data fiduciaries or data processors with whom data may be shared, if applicable;

g) The period of time for which the data shall be retained, or where the period of retention is not known, then the criteria for determining such period;

h) The contact details and the mechanism by which the farmer may contact the data fiduciary in relation to complaints, inquiries, and clarifications regarding the policies, practices and procedures employed in the collection, storage, transmission or any other aspect of processing of data.

4.3. The privacy notice shall be clear, concise and easily comprehensible to a reasonable person and shall be available in English and local languages. Such notice may also be made available over audio medium, considering the convenience of those who are visually impaired.

5. Method of Obtaining Consent

5.1. The consent of the farmer, as referred to in Clauses 3 and 4 of this Policy, for collection, or further processing of personal data, may be obtained electronically (Figure 2) or via the Mo Seba Kendra (MSK)/Common Services Center (CSC)/Government extension worker, as the case may be. Where the consent is received via a government intermediary, then in this case the farmer is deemed to have given consent to the sharing and processing of their data by the data fiduciary as per the provisions under chapter 2 (Deemed Consent) of DPDP Act- 2023. In accordance with the IT Act, all state of the art security practices will be followed when obtaining consent electronically.

5.2. Where consent is obtained through a government intermediary, as set out above then such centers or individuals shall not access, process or store, in any manner whatsoever, the data shared with any data fiduciary.

5.3. Where the farmer has revoked his/her consent, it shall be the duty of the MSK/CSC/Govt. Extension Worker to notify the data fiduciary of such revocation, as applicable. In accordance with the DPDP Act, to maintain transparency, farmers must be able to revoke or withdraw consent easily.

5.4. Aadhaar Act: For consent obtained through Government intermediaries, it is to be ensured that Aadhaar data is not accessed or used without meeting stringent consent requirements set by the Aadhaar Act.

6. **Transparency and Accountability Measures**

   6.1. **Reasonable Security Practices and Procedures**

   a) The data fiduciaries will implement reasonable security practices and standards and have a comprehensive documented information security programme and information security policy that contain managerial, technical, operational and physical security control measures that are commensurate with the data/information assets being protected by them.

   b) In the event of a data/information security breach, the data fiduciary shall be required to demonstrate, as and when called upon to do so by any agency mandated under the law (Data Protection Board of India as established by DPDP Act, 2023), that they have implemented security control measures as per their documented information security programme and information security policies.

   c) The data fiduciaries will, having regard to the nature, scope and purpose of processing data, the risks associated with such processing, and the likelihood and severity of harm that may result from such processing, implement necessary security safeguards including the use of de-identification and encryption methods, methods to protect the integrity of the data collected, and methods to prevent misuse, unauthorized access to, modification, disclosure or destruction of data. Every data fiduciary shall undertake a review of its security safeguards in a periodic manner and take appropriate measures accordingly.

   d) In the case of any entities who are implementing/involved in the KONNECT stack and acting as a data fiduciary in this regard, the DAFE will undertake a periodic review of the security safeguards and take appropriate measures to update such safeguards, if required.

6.2. Maintenance of Records:

    a) The data fiduciaries will maintain accurate and up-to-date records to document the important operations in the data lifecycle including collection, transfers, and erasure of obtained data. These will cover the following:

        i.   Details of the ecosystem partners.
        ii.   Purposes of the processing.
        iii. Description of the categories of personal and sensitive data.
        iv. Categories of recipients to whom the data is disclosed/transferred.

    b) In addition to the records referred to above and elsewhere in this framework, the data fiduciaries will also maintain accurate and up-to-date records of the periodic review of security safeguards conducted under Clause 6.1 of this framework.

7. Data Protection Officer (DPO) and Regulatory Oversight:

An officer from the department of agriculture and farmers' empowerment will be appointed by the competent authority as a Data Protection Officer for overseeing data protection and compliance with the DPDP Act. In accordance with the IT Act, any incident or breach will be notified by the DPO to the competent authority with a detailed root cause analysis and solution to rectify the breach/incident. Platforms that use Aadhaar data (e.g.Krushak Odisha, etc), must be under oversight of UIDAI and relevant regulatory reporting authorities.

8. Anonymization:

The anonymization process within the agri data exchange module of consent manager will comply with standards of irreversibility and data protection, as required by respective relevant laws.

9. Data Portability and Erasure:

Farmers will be provided with the option to access their data and request its deletion or portability, as per the provisions outlined in DPDP Act.

10. Cross Border Data Transfer:

If any data transfer across international borders is involved, the data sharing mechanism proposed will comply with regulations on international data transfer as provisioned in the DPDP Act.

Conclusion:

The data sharing framework is formulated with a mandate of using farmer data by ecosystem partners in a secured and private manner for their welfare. This framework will act as an enabler for bringing the markets closer to the farmers, thereby leading to easy and speedy delivery of services to farmers by ecosystem partners. Using this framework, the department on one hand can provide a single unified system to farmers but also on the other hand protect the privacy of the

farmers, keeping them away from unintentional harm that may arise due to unauthorized proliferation of personal data. The scope and objectives may be expanded and enriched in future, as the data sharing technologies and protocols keep evolving day-by-day in the industry.

By Order of the Governor
ARABINDA KUMAR PADHEE
Principal Secretary to Government

————